Federal Deposit Insurance Corporation
801 17th Street NW, Washington DC 20434
Office of Inspector General

DATE: December 16, 2004

MEMORANDUM TO: Board of Directors

FROM: Gaston L. Gianni, Jr.
Inspector General

SUBJECT: OIG's Assessment of the Management and Performance Challenges Facing the FDIC

In the spirit of the Reports Consolidation Act of 2000 (Act), we are providing you with the Office of Inspector General's (OIG) assessment of the most significant management and performance challenges (MPCs) facing the FDIC. The Act calls for these challenges to be included in the consolidated performance and accountability reports of those federal agencies to which it applies. We will also provide (1) the attachment to the Chief Financial Officer and (2) a summary of the challenges to the Office of Enterprise Risk Management for inclusion in the 2004 Annual Report. The seven challenges we have identified are listed in priority order. In the past two years, we identified 10 MPCs. This year we consolidated a number of MPCs into "Corporate Governance in the FDIC" and introduced "Money Laundering and Terrorist Financing" as a new MPC.

We shared a draft listing of the MPCs with the divisions and offices. We also briefed the Audit Committee on December 9, 2004. We appreciate the cooperation and coordination of the divisions and offices in formulating our assessment. Their comments on the challenges attest to the fact that the Corporation has a number of actions under way to address many of the issues, and we encourage continued attention to each challenge. For its part, the OIG will continue to add value by conducting audits, evaluations, investigations, and other reviews that address the challenges. We look forward to working with you and others in the Corporation on these efforts.

If you have any questions or need additional information, please feel free to contact me at 202-416-2026.

Attachment

cc: Walter B. Mason
Thomas Zemke
John F. Bovenzi, COO
Steve O. App, CFO
Michael E. Bartell, CIO

OIG's Assessment of the Management and Performance Challenges Facing the FDIC

DETAILED NARRATIVE

1. Corporate Governance in Insured Depository Institutions
2. Management and Analysis of Risks to the Insurance Funds
3. Security Management
4. Money Laundering and Terrorist Financing
5. Protection of Consumers' Interests
6. Corporate Governance in the FDIC
7. Resolution and Receivership Activities

1. Corporate Governance in Insured Depository Institutions

Corporate governance is generally defined as the fulfillment of the broad stewardship responsibilities entrusted to the Board of Directors, officers, and external and internal auditors of a corporation. A number of well-publicized announcements of business and accountability failings, including those of financial institutions, have raised questions about the credibility of management oversight and accounting practices in the United States. In certain cases, board members and senior management engaged in high-risk activities without proper risk management processes, did not maintain adequate loan policies and procedures, and circumvented or disregarded various laws and banking regulations. In an increasingly consolidated financial industry, effective corporate governance is needed to ensure adequate stress testing and risk-management processes covering the entire organization. Adequate corporate governance protects the depositor, institution, nation's financial system, and FDIC in its role as deposit insurer. A lapse in corporate governance can lead to a rapid decline in public confidence, with potentially disastrous results to the institution.

In some cases, a dominant official exercised undue control over bank operations--to the bank's detriment. In other cases, independent public accounting firms rendered clean opinions on institutions' financial statements when, in fact, the statements were materially misstated. These events have increased public concern regarding the adequacy of corporate governance and, in part, prompted passage of the Sarbanes-Oxley Act of 2002 (SOX). This Act has focused increased attention on management assessments of internal controls over financial reporting and the external auditor attestations of these assessments. Strong stewardship along with reliable financial reports from insured depository institutions are critical to FDIC mission achievement. Supervision and insurance aspects of the Corporation's mission can be complicated and potentially compromised by poor quality financial reports and audits. In the worst case, illegal and otherwise improper activity by management of insured institutions or their boards of directors can be concealed, resulting in potential significant losses to the FDIC insurance funds.

The FDIC has initiated various measures designed to mitigate risks posed by these concerns, such as reviewing the bank's board activities and ethics policies and practices and reviewing auditor independence requirements. In fact, many of the SOX requirements parallel those already applicable to insured depository institutions. The FDIC also reviews the publicly traded banks' compliance with Securities and Exchange Commission regulations and the approved and recommended policies of the Federal Financial Institutions Examination Council (FFIEC) to help ensure accurate and reliable financial reporting through an effective external auditing program and on-site FDIC examination. Other corporate governance initiatives include issuing Financial Institution Letters, allowing bank directors to participate in regular meetings between examiners and bank officers, maintaining a "Directors' Corner" on the FDIC Web site, and expanding the Corporation's "Directors' College" program, as well as plans for expanding examiner guidance on the risks posed by dominant officials. The FDIC has taken significant strides; however, achieving sound corporate governance without undue regulatory burden remains a management challenge.

The assessment of management is one of the most important aspects of a bank examination. Failure to appropriately evaluate management risks increases the opportunity for fraud or mismanagement to go undetected and uncorrected and could ultimately cause an institution to fail. Independent boards of directors, effective security programs, and strong commitments to sound internal control and compliance with laws and regulations all complement the FDIC's supervision and monitoring of insured depository institutions.

2. Management and Analysis of Risks to the Insurance Funds

A primary goal of the FDIC under its insurance program is to ensure that its deposit insurance funds do not require augmentation by the U.S. Treasury. Achieving this goal is a considerable challenge that requires effective communication and coordination with the other federal banking agencies. The FDIC engages in an ongoing process of proactively identifying risks to the deposit insurance funds and adjusting the risk-based deposit insurance premiums charged to the institutions.

Recent trends and events continue to pose risks to the funds. The consolidations that have and may continue to occur among banks, securities firms, insurance companies, and other financial services providers resulting from the Gramm-Leach-Bliley Act (GLBA) pose increasing risks to the FDIC's insurance funds. The bank mergers have created "large banks," which are generally defined as institutions with assets of over $25 billion. For many of these institutions, the FDIC is the insurer but is not the primary federal regulator. In addition, the FDIC is the primary federal regulator for a number of industrial loan companies (ILCs), which are insured depository institutions owned by organizations that are subject to varying degrees of federal regulation. ILC charters allow mixing of banking

and commerce which is otherwise prohibited for most other depository institutions owned by commercial firms. The FDIC has instituted controls in its processes for deposit insurance applications, safety and soundness examinations, and offsite monitoring for supervising ILCs and their parent companies, particularly in cases where consolidated supervision is not provided by another federal regulator.

Failure of a large bank, along with the potential closing of closely affiliated smaller institutions, could result in losses to the deposit insurance funds that require significant increases in premium assessments from all insured institutions. To address the risks associated with large banks for which the FDIC is the insurer but is not the primary federal regulator, the FDIC initiated, in 2002, the Dedicated Examiner Program for the largest banks in the United States. One senior examiner from the FDIC is dedicated to each institution and participates in targeted reviews or attends management meetings. Additionally, case managers closely monitor such institutions through the Large Insured Depository Institutions Program's quarterly analysis and executive summaries. These case managers also consistently remain in communication with their counterparts at the other regulatory agencies, frequently attending pre-examination meetings, post-examination meetings, and exit board meetings.

Large banks may pose greater risks to the insurance funds as a result of the Basel II capital accord, which aims to align capital reserves more closely with the risks faced by banks and thrifts operating internationally. The Basel II standard is mandatory for large internationally active banks that have either total commercial bank assets of $250 billion or more or foreign exposure of $10 billion or more. As of October 2004, Basel II will be mandatory for 10 FDIC-insured banks. In addition, 20 other banks have shown interest in opting in to the Basel II standard requirements. Basel II will have far-reaching effects on the management and supervision of the largest, most complex banking organizations in the world. The United States has an important role in Basel II implementation because it supervises more bank assets than the other accord participants. Issues that must be addressed before the United States implements the Basel II accord are: (1) assuring appropriate minimum capital standards for banks regardless of the results of proposed capital models, (2) establishing a consistent supervisory process for ensuring that banks' internal risk estimates are sound and conservative, and (3) vetting any potential anti-competitive effects with all interested parties.

There is ongoing consideration to merging the Bank Insurance Fund (BIF) and Savings Association Insurance Fund (SAIF) in the hope that the merged fund would not only be stronger and better diversified but would also eliminate the concern about a deposit insurance premium disparity between the BIF and the SAIF. Assessments in the merged fund would be based on the risk that institutions pose to that fund. The prospect of different premium rates for identical deposit insurance coverage would be eliminated. The Corporation has worked hard to bring about deposit insurance reform, and the OIG supports the FDIC's continued work with the banking community and the Congress in the interest of eventual passage of reform legislation.

As the banking industry has become more sophisticated, the FDIC has developed cutting edge risk-management techniques to identify, measure, and manage risk to the insurance funds. In 2003 the FDIC created its Risk Analysis Center (RAC) to better coordinate risk monitoring and action plans among the various business units in the FDIC. The RAC represents a best practice that brings together economists, examiners, financial analysts, and others involved in assessing risk to the banking industry and the deposit insurance funds.

3. Security Management

The FDIC relies heavily upon automated information systems to collect, process, and store vast amounts of banking information. This information is used by financial regulators, academia, and the public to assess market and institution conditions, develop regulatory policy, and conduct research and analysis on important banking issues. Ensuring the confidentiality, integrity, and availability of this information in an environment of increasingly sophisticated security threats requires a strong, enterprise-wide information security program at the FDIC and insured depository institutions. It also requires compliance with applicable statutes and policies aimed at promoting information security throughout the federal government. One such statute is Title III of the E-Government Act of 2002, commonly referred to as the Federal Information Security Management Act of 2002 (FISMA).

As a result of focused efforts over the past several years, the FDIC has made significant progress in improving its information security controls and practices and addressing current and emerging information security requirements mandated by FISMA. However, the FDIC recognizes that continued improvements in its information security program and practices are needed. In its 2003 annual report to the Congress, the FDIC identified information security as a high vulnerability issue within the Corporation. The FDIC also identified improvements in its information security program as a major corporate priority in its *2004 Annual Performance Plan*.

Although progress in strengthening the FDIC's information security program and practices has been notable, additional control improvements and associated implementation activities would help ensure that the FDIC reaches a superior level of security assurance. Continued management attention is needed to ensure that the FDIC's information security risk management program and practices are consistent with National Institute of Standards and Technology (NIST) standards and guidance and current best practices in the industry. The FDIC would benefit from enhanced oversight of contractors with access to sensitive data, implement additional measures to ensure the security of its network resources, and efforts to ensure that its enterprise security architecture is fully defined and integrated with corporate business and information technology operations. Additional security-related threats include those focusing on disrupting the economic security of our nation. The FDIC and insured depository institutions need to ensure that sound disaster recovery and

business continuity planning is present to safeguard depositors, investors, and others who depend on the financial services.

4. Money Laundering and Terrorist Financing

The nation faces a new and changing threat unlike any we have faced before -- the global threat of terrorism. In response to this threat, the Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law 107-56 (USA PATRIOT Act), which expands the Treasury Department's authority initially established under the Bank Secrecy Act of 1970 (BSA) to regulate the activities of U.S. financial institutions, particularly their relations with individuals and entities with foreign ties.

Specifically, the USA PATRIOT Act expands the BSA beyond its original purpose of deterring and detecting money laundering to also address terrorist financing activities. In today's global banking environment, where funds are transferred instantly and communication systems make services available internationally, a lapse at even a small financial institution outside of a major metropolitan area may have larger implications. The reality today is that all institutions are at risk of being used to facilitate criminal activities, including terrorist financing.

Through its examiners, the FDIC seeks to ensure that institutions have a strong BSA program to address money laundering and terrorist financing concerns. While many FDIC-supervised institutions are diligent in their efforts to establish, execute, and administer effective BSA compliance programs, the FDIC has identified instances where controls and efforts were lacking. In such cases, the FDIC may request bank management to address the deficiencies in a written response to the FDIC, outlining the corrective action proposed and establishing a timeframe for implementation, or the FDIC may pursue an enforcement action. The FDIC needs to strengthen its follow-up process for BSA violations. The FDIC is taking action to expand its pool of BSA specialists, ensure adequate coverage of BSA compliance in state examinations, and update its policies and procedures.

In addition, in September 2004, the Financial Crimes Enforcement Network (FinCEN), an arm of the U.S. Treasury Department, signed an information-sharing Memorandum of Understanding (MOU) with the Federal Banking Agencies (FBAs), including the FDIC. The MOU requires an increased level of BSA reporting and accountability between the FBAs and FinCEN. Specifically, the FBAs will notify FinCEN of significant violations of BSA laws and regulations by institutions, enforcement actions taken, and resolution of enforcement actions. Similarly, FinCEN, based on its analyses of BSA violations, will notify FBAs of common BSA compliance deficiencies, patterns, and best practices; and assist FBAs in identifying BSA compliance deficiencies within banking organizations.

The continuing challenge facing the FDIC is to ensure that banks maintain effective BSA programs that will ultimately create an environment where attempts to use the American financial system for money laundering or terrorist financing will be identified and ultimately thwarted.

5. Protection of Consumers' Interests

In addition to its mission of maintaining public confidence in the nation's financial system, the FDIC also serves as an advocate for consumers through its oversight of a variety of statutory and regulatory requirements aimed at protecting consumers from unfair and unscrupulous banking practices. The FDIC is legislatively mandated to enforce various statutes and regulations regarding consumer protection and civil rights with respect to state-chartered, non-member banks and to encourage community investment initiatives by these institutions. Ensuring the protection of consumer interests is a major challenge in an environment of increasingly large financial institutions that lack the historic geographic boundaries or operations and offer an increasing array of consumer products.

The FDIC accomplishes its mission of protecting consumers under various laws and regulations by conducting compliance examinations and Community Reinvestment Act (CRA) evaluations. The FDIC takes enforcement actions to address compliance violations, encourages public involvement in the community reinvestment process, assists financial institutions with fair lending and consumer compliance through education and guidance, and provides assistance to various parties within and outside of the FDIC. The Corporation has also developed a program to examine institution compliance with privacy laws.

The FDIC also has a Community Affairs program that provides technical assistance to help banks meet their responsibilities under the CRA. One current emphasis is on financial literacy, aimed specifically at low- and moderate-income people who may not have had banking relationships. The Corporation's "Money Smart" initiative is a key outreach effort. The FDIC also continues to maintain a Consumer Affairs program by investigating consumer complaints against FDIC-supervised institutions, answering consumer inquiries regarding consumer protection laws and banking practices, and providing data to assist the examination function. Further, the Corporation's deposit insurance program promotes public understanding of the federal deposit insurance system and seeks to ensure that depositors and bankers have ready access to information about the rules for FDIC insurance coverage.

Protecting consumers from unscrupulous banking practices also continues to be a challenge. For example, "predatory lenders" knowingly lend more money than a borrower can afford to repay; charge high interest rates to borrowers based on their race or national origin and not on their credit history; charge fees for unnecessary or nonexistent products and services; pressure borrowers to accept higher-risk loans such as balloon loans, interest-only payments, and steep pre-payment penalties; and "strip" homeowners' equity

by convincing them to refinance again and again when there is no benefit to the borrower. These practices ultimately put borrowers at risk of losing their homes and other investments.

A number of new consumer protection regulations have been introduced over the past several years. The emergence and continued expansion of electronic banking presents a challenge for ensuring that consumers are protected. The number of reported instances of identity theft has ballooned in recent years. The Corporation will need to remain vigilant in conducting comprehensive, risk-based compliance examinations that ensure the protection of consumer interests, analyzing and responding appropriately to consumer complaints, and educating individuals on money management topics, including identity protection and how to avoid becoming victims of "phishing" scams.[1] In addition, the Corporation will need to remain diligent in its efforts to work with the other federal banking regulators to develop uniform policy changes for CRA. A challenge facing the FDIC and other regulators is protecting of consumer interests while minimizing regulatory burden.

6. Corporate Governance in the FDIC

Corporate governance within the FDIC is the responsibility of the Board of Directors, officers, and operating managers in fulfilling the Corporation's broad mission functions. It also provides the structure for setting goals and objectives, the means to attaining those goals and objectives, and ways of monitoring performance. Management of the FDIC's corporate resources is essential for efficiently achieving the FDIC's program goals and objectives.

Also, the administration has outlined management initiatives for departments and major agencies in the President's Management Agenda (PMA). These initiatives are (1) strategic management of human capital, (2) competitive sourcing, (3) improved financial management, (4) expanded electronic government, and (5) budget and performance integration. Although the FDIC is not subject to the PMA, it has given priority attention to continuing efforts to improve operational efficiency and effectiveness, consistent with the PMA. The initiatives taken and opportunities for improvement are discussed below along with other issues that pose significant elements of risk to attaining the FDIC's program goals and objectives:

a. Management of Human Capital. The FDIC, like other organizations, continues to be affected by changing technology, market conditions, initiatives designed to improve its business processes, an aging workforce, and the unknown. Such events impact needed staffing levels and required skills going forward. Since 2002, the FDIC has been

[1] Phishing scams use e-mails and Web sites to fool recipients into revealing financial data, such as credit card and Social Security numbers.

working to create a flexible permanent workforce that is poised to respond to sudden changes in the financial sector. Recently, FDIC executives announced workforce planning initiatives providing for human resources flexibilities, the establishment of a Corporate Employee Program, a Buyout Program, and possible reductions-in-force. Designing, implementing, and maintaining effective human capital strategies—including developing a coherent human capital blueprint that comprehensively describes the FDIC's human capital framework and establishes a process for agency leaders to systematically monitor the alignment and success of human resources-related initiatives —are critical priorities and must continue to be the focus of centralized, sustained corporate attention. The FDIC's training and development function, known as the FDIC Corporate University, will be a key ingredient in the successful implementation of the FDIC's Corporate Employee Program and other corporate efforts to address skill and competency requirements.

b. Competitive Sourcing. The FDIC is in the process of awarding long-term contracts to consolidate outsourced information technology activities. While these contracts will permit the FDIC to solicit among well-qualified sources under task orders, the FDIC's ability to compete will generally be limited to a small number of firms. Attaining the desired services at competitive prices will present a significant challenge for the FDIC.

c. Improved Financial Management. The FDIC plans to field a new financial management system in 2005 that will consolidate the operations of multiple systems. Named the New Financial Environment (NFE), this initiative will modernize the FDIC's financial reporting capabilities. Implementing NFE and interfacing other systems with NFE will require significant efforts and poses major challenges.

d. E-Government. The FDIC's E-Government Strategy is a component of the enterprise architecture that focuses on service delivery for the external customers of the FDIC. The FDIC issued Version One of its E-Government Strategy in November 2002 and is in the process of establishing a task force to update the strategy. The FDIC has initiated a number of projects that will enable the Corporation to improve internal operations, communications, and service to members of the public, businesses, and other government offices. The projects include: Call Report Modernization, Virtual Supervisory Information on the Net, Asset Servicing Technology Enhancement Project, New Financial Environment, Corporate Human Resources Information System, and FDIConnect. The risks of not implementing e-government principles are that the FDIC will not efficiently communicate and serve its internal and external customers.

e. Risk Management and Assessment of Corporate Performance. Within the business community, there is a heightened awareness of the need for a robust risk management program. Because of past corporate governance breakdowns at some major corporations, organizations are seeking a "portfolio" view of risks and the launch of proactive measures against threats that could disrupt the achievement of strategic goals and objectives. To address these needs, a best practice has developed--enterprise risk

management (ERM). ERM is a process designed to: identify potential events that may affect the entity, manage identified risks, and provide reasonable assurance regarding how identified risks will affect the achievement of entity objectives. In April 2004, the FDIC's Chief Financial Officer changed the name of the Office of Internal Control Management to the Office of Enterprise Risk Management (OERM) and the OERM has begun developing an ERM program for the FDIC. The migration from internal control to enterprise risk management perspectives and activities presents challenges and opportunities for the FDIC.

In the spirit of the Government Performance and Results Act of 1993, the FDIC prepares a strategic plan that outlines its mission, vision, and strategic goals and objectives within the context of its three major business lines; an annual performance plan that translates the vision and goals of the strategic plan into measurable annual goals, targets, and indicators; and an annual performance report that compares actual results against planned goals. In addition, the FDIC Chairman develops a supplemental set of "stretch" annual corporate performance objectives based on three strategic areas of focus that cut across the Corporation's three business lines: Sound Policy, Stability, and Stewardship. The Division of Finance monitors the Corporation's success in meeting both sets of performance objectives and develops quarterly reports on the FDIC's progress. Executive and managerial pay are linked to performance on both the Chairman's objectives and those in the annual performance plan.

The Corporation is continually focused on establishing and meeting annual performance goals that are outcome-oriented, linking performance goals and budgetary resources, implementing processes to verify and validate reported performance data, and addressing cross-cutting issues and programs that affect other federal financial institution regulatory agencies.

f. Security of Critical Infrastructure. To effectively protect critical infrastructure, the FDIC's challenge in this area is to implement measures to mitigate risks, plan for and manage emergencies through effective contingency and continuity planning, coordinate protective measures with other agencies, determine resource and organization requirements, and engage in education and awareness activities. The FDIC will need to continue to work with the Department of Homeland Security and the Finance and Banking Information Infrastructure Committee, created by Executive Order 23231 and chaired by the Department of the Treasury, on efforts to enhance security of the critical infrastructure of the nation's financial system. To address this risk, the FDIC is sponsoring outreach conferences for the Financial and Banking Information Infrastructure Committee and Financial Services Sector Coordinating Council through 2005, which will address protecting the financial sector.

OIG's Assessment of the Management and Performance Challenges Facing the FDIC

On December 17, 2003, the President signed Homeland Security Presidential Directive (HSPD)–7, *Critical Infrastructure Identification, Prioritization and Protection.* HSPD–7 established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist acts. On June 17, 2004, the Office of Management and Budget (OMB) issued Memorandum M-04-15, *Development of the HSPD-7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources*. The memorandum provides guidance regarding the format and content of critical infrastructure protection plans that federal agencies are required to submit to the OMB. Although the FDIC has determined that it does not maintain critical infrastructure or key resources as intended by HSPD–7, the FDIC is required to report to OMB on its ability to ensure the continuity of its business operations in the event of a physical or cyber attack. The FDIC provided its Critical Infrastructure Protection plan to OMB in August 2004. However, the FDIC will need to ensure that the Plan is kept current and up-to-date, particularly in light of transformation activities in the Division of Information Resources Management.

With respect to IT contingency planning, the FDIC has continued capability to recover its mainframe and server platforms necessary to restore operations in the event of a disaster. However, testing for data restoration is one area needing improvement. While, the FDIC's Business Continuity Plan (BCP) addresses critical business functions in key divisions and offices, identifies that actions are underway to review and update a business impact analysis, and outlines the resources necessary to sustain essential functions in the event of disruptions, the FDIC could improve the quality of its BCP in a number of key areas to help ensure the plan's success. Also, continued testing and updates of the plan must be part of a sound BCP process.

g. Management of Major Projects. Project management involves defining, planning, scheduling, and controlling the tasks that must be completed to reach a goal and allocating resources to perform those tasks. The FDIC has engaged in several multi-million dollar projects, such as the NFE, Central Data Repository, and Virginia Square Phase II Construction. Without effective project management, the FDIC runs the risk that corporate requirements and user needs may not be met in a timely, cost-effective manner. In September 2002, the FDIC established the Capital Investment Review Committee (CIRC) as the control framework for determining whether a proposed investment is appropriate for the FDIC Board of Directors' consideration, overseeing approved investments throughout their life cycle, and providing quarterly capital investment reports to the Board. The CIRC generally monitors projects valued at more than $3 million. The FDIC also developed the Chief Information Officers (CIO) Council to recommend and oversee technology strategies, priorities, and progress. The work of the Council encompasses the entire portfolio of technology projects, including those below the threshold addressed by the CIRC.

Beginning with the 2003 budget, the FDIC began budgeting and tracking capital investment expenses as a separate component of the budget to enhance management's ability to focus on such projects. Project funds established within the investment budget are to be available for the life of the project rather than for the fiscal year. Final responsibility for approving the initial creation or modification of a project's capital investment budget rests with the FDIC's Board of Directors. In addition, the Division of Information Resources Management has recently adopted the Rational Unified Process system development life cycle model and has established a Project Management Office. Both of these initiatives should result in additional oversight and control mechanisms for corporate projects.

The FDIC's System Development Life Cycle (SDLC) methodology and the related control framework can benefit from implementing identified best practices. The FDIC has selected a risk-based SDLC methodology and developed a statement of work to implement the new methodology. Also, issuing detailed IT enterprise architecture guidance can help implement higher-level policy and general guidance. As these initiatives are addressed, the FDIC should promptly implement the necessary control framework. Doing so would provide the Corporation with greater assurance that major projects meet cost, schedule, and quality goals; the development process continually improves; all system development projects are consistent with the FDIC enterprise architecture; and effective security controls exist in all completed systems.

h. Cost Containment and Procurement Integrity. As steward for the BIF, SAIF, and FSLIC Resolution Fund (FRF), the FDIC strives to identify and implement measures to contain and reduce costs, either through more careful spending or by assessing and making changes in business processes to increase efficiency. A key challenge to containing costs relates to the contracting area. To assist the Corporation in accomplishing its mission, contractors provide services in such areas as information technology, legal matters, loan servicing, and asset management. To contain costs, the FDIC must ensure that its acquisition framework—its policies, procedures, and internal controls—is marked by sound planning; consistent use of competition; fairness; well-structured contracts designed to result in cost-effective, quality performance from contractors; and vigilant oversight management to ensure the receipt of goods and services at fair and reasonable prices.

7. Resolution and Receivership Activities

One of the FDIC's responsibilities is planning and efficiently handling the franchise marketing of failing FDIC-insured institutions and providing prompt, responsive, and efficient resolution of failed financial institutions. These activities maintain confidence and stability in our financial system.

OIG's Assessment of the Management and Performance Challenges Facing the FDIC

The Division of Resolutions and Receiverships (DRR) has outlined primary goals for three functional areas (listed below) that are relevant to the three major phases of its work: Pre-Closing, Closing, and Post-Closing of failed institutions. Each is accompanied by significant challenges:

a. Deposit Insurance. The FDIC must provide customers of failed financial institutions with timely access to their insured funds and financial services. A significant challenge in this area is to ensure that FDIC deposit insurance claims and payment processes are prepared to handle large institution failures.

b. Resolutions. As the FDIC seeks to resolve failing institutions in the least costly manner, its challenges include improving the efficiency of contingency planning for institution failures and ensuring effective internal FDIC communication and coordination as well as communication with the other primary federal regulators.

c. Receivership Management. Related challenges include ensuring the efficiency and effectiveness of the receivership termination process and claims processing, continually assessing recovery strategies and investigative activities, collecting restitution orders, and charging receiverships for services performed under the Receivership Management Program.

In addition to the challenges inherent in the three major phases of DRR work, DRR faces other challenges from a significant downsizing of its current staffing levels and from an ambitious information system enhancement project, the Asset Servicing Technology Enhancement Project (ASTEP), which is intended to create an integrated solution to meet the FDIC's current and future asset servicing responsibilities based on industry standards, best practices, and adaptable technology. Successfully implementing ASTEP is an important component of DRR's mission achievement.